Department of Homeland Security Daily Open Source Infrastructure Report for 18 July 2006

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- Reuters reports that according to utility and power grid operators, blistering temperatures from New York to Sacramento will boost power demand this week to record highs and strain electric resources across the U.S. as people try to escape the sweltering heat. (See item 1)
- The Boston Globe reports another crucial link between Interstates 90 and 93 in the heart of Boston has been closed after inspectors found about 40 potentially dangerous bolt fixtures similar to the ones suspected in last week's fatal tunnel ceiling collapse. (See item 12)
- The Department of Homeland Security along with a coalition of more than 200 national, regional, state, and local organizations will sponsor National Preparedness Month in September to encourage Americans to prepare for emergencies in their homes, businesses, and schools. (See item 29)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *July 18, Reuters* — **U.S. sees widespread record power use amid heat wave.** Blistering temperatures from New York to Sacramento will boost power demand this week to record highs and strain electric resources across the U.S. as people try to escape the sweltering heat,

according to utility and power grid operators. PJM Interconnection, asked customers in Pennsylvania, Maryland, and New Jersey to conserve energy for the next few days as demand could reach an all−time high of 138,000 megawatts, breaking the current record of 133,763 MW set on July 26, 2005. The New York Independent System Operator forecast peak demand would hit 33,000 MW, breaking its all−time high of 32,075 MW on July 26. The Midwest Independent Transmission System Operator forecast demand of 115,400 MW, above the 2005 peak of 112,197 MW, while in California, the state grid operator forecast demand to rise to a record of 47,050 MW, up from 45,431 MW. Texas was expected to set a fourth record for the month with demand to exceed 63,000 MW, topping the 2005 all−time peak of 60,274 MW.
Source: http://news.yahoo.com/s/nm/20060717/us_nm/utilities_demand_h eatwave_dc_1

2. *July 17, Associated Press* — **Fire extinguished at Venezuelan refinery.** A fire broke out early Monday, July 17, at a major oil refinery in western Venezuela, but it was extinguished without reported injuries or loss of deliveries, officials said. The fire began in the distillation unit of the 635,000 barrel−a−day Amuay refinery, said state oil company Petroleos de Venezuela SA (PDVSA). PDVSA said the unit affected produces 190,000 barrels a day, but that the rest of the refinery was operating normally. Oil deliveries to the international and domestic markets would not be affected, PDVSA said. The Amuay refinery has suffered a series of problems in recent months. The refinery's manager, Jesus Luongo, said PDVSA has spent more than $160 million to improve safety at the installation in response to the string of accidents, contracting DuPont Co., which gave 290,000 hours of safety−related training to workers last year. Venezuela is consistently among the top five suppliers of crude to the U.S.
Source: http://www.oregonlive.com/newsflash/international/index.ssf?/base/international−8/1153159165201160.xml&storylist=orinter national

3. *July 16, BBC* — **G8 supports open energy markets.** Russia has taken a step towards opening its energy sector to foreign investment at the G8 meeting in St Petersburg. The group agreed to "open, transparent" energy markets and to nuclear energy as a power source for those who want it. G8 leaders did express, in principle, their support for the Energy Charter treaty, which calls for open access to energy resources and transport infrastructure. The European Union has been pressing Russia, which supplies a quarter of the continent's gas, to fully ratify the charter which it has signed. The UK government recently announced the go−ahead for a new wave of UK nuclear power stations, as part of the mix of energy supply for the next 40 years. Most G8 countries have been looking again at the development of nuclear energy as an alternative to fossil fuels, but Germany is not supportive and plans to phase out nuclear energy by the early 2020s.
Source: http://news.bbc.co.uk/2/hi/business/5184776.stm

4. *July 14, Charlotte Observer (NC)* — **Number of natural gas line breaks on the rise.** Three gas lines were cut Thursday, July 13, amid construction projects around Charlotte, NC, according to the fire department. That's more then usual for an average day, city records show, but the number of such potentially deadly mistakes has been on the rise. The Charlotte Fire Department responded to 41 percent more natural gas line breaks in the past year than just two years ago, up to 276 from 196, said Capt. Rob Brisley. Those leaking pipes can lead to traffic tie−ups, evacuations, and even deadly explosions.
Source: http://powermarketers.netcontentinc.net/newsreader.asp?ppa=8knpp%5E%5BigjoqqkRTif%7DGJ%7Bbfel%5Dv

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

5. *July 16, Aviation Week* — **Industry, government make renewed push to change U.S. export control regime.** With industry concerns growing that the arms export control system is hurting business and hampering cooperation with foreign partners, advocates of reform are coalescing around plans for a renewed push to change. Under current law, export controls are delegated to the State Department, whose Office of Defense Trade Controls is responsible for processing export licenses. With the end of the Cold War, industry and government officials alike felt there was a need to reform a system that many felt took too long, tried to control too much and was aimed at a problem that no longer existed: trying to keep advanced technology out of the hands of the Soviet Union. Everyone involved in the export debate agrees −− to some degree −− that the licensing process could and should work better. One of the lessons, however, is that good intentions aren't enough −− reforms have to be workable, and perhaps even more important, they have to be agreeable to all sides. That understanding has led many to advocate a new approach: start with improving the current system, and then work for bigger changes.
Source: http://www.aviationnow.com/avnow/news/channel_awst_story.jsp?id=news/aw071706p1.xml

[Return to top]

Banking and Finance Sector

6. *July 15, Reuters* — **IMF warns of fake e−mails using its name.** The International Monetary Fund (IMF) on Friday, July 14, warned of a jump in the number of fraudulent e−mails and communications claiming to be from or affiliated with the lender. There has been an apparent spike in such messages recently involving people in the U.S. targeting recent immigrants and people in cities, an IMF official said. U.S. authorities have been informed. The scams include phishing attacks where the names of IMF officials are misused to deceive recipients into disclosing personal financial information to spoofing, in which a fake IMF Website was created with false contact details to mislead potential users.
Source: http://news.com.com/IMF+warns+of+fake+e−mails+using+its+name/2100−7349_3−6094634.html?tag=cd.top

7. *July 15, Consumer Affairs* — **Michigan warns of advance fee loan scams.** Michigan Attorney General Mike Cox is warning consumers that advance−fee loan crooks are using false Michigan business addresses and targeting people with debt problems through Websites. Cox highlighted recent complaints regarding the Royal Oak Financial Group and SouthField Financial Group, both of whom falsely claim to be headquartered in Michigan. Recent complaints and calls

received by Cox's office evidence consumers who wired hundreds of dollars in up−front fees to secure personal loans but then failed to receive either the loan proceeds or payment refunds. After applying for a loan online through the Website of Royal Oak Financial Group, consumers were directed to pay upfront for insurance by wire transfer to Canada and directed to a named individual, rather than the company name.
Source: http://www.consumeraffairs.com/news04/2006/07/mi_advance_fee .html

8. *July 15, Forum of Incident Response and Security Teams* — **Report: Treasury's Terrorist Finance Program's Access to Information Held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).** Recent press reports have raised questions about the Department of the Treasury's Terrorist Finance Tracking Program's access to information on international financial transactions held by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), an organization owned by banks in many countries, which serves as a hub for international funds transfers. Its records contain names, addresses, and account numbers of senders and receivers of international wire transfers between banks and between securities firms, thus providing a useful source for federal officials responsible for following money trails across international borders. On June 29, 2006, the House of Representatives passed H.Res. 895 voicing support for the Treasury program as fully compliant with all applicable laws; condemning the unauthorized disclosure of classified information; and calling upon news media organizations not to disclose classified intelligence programs. H.Res. 904 was introduced to discourage government censorship of the press. This report addresses these issues and will be updated as legislative events merit.
Report: http://www.fas.org/sgp/crs/natsec/RS22469.pdf
Source: https://www.first.org/newsroom/globalsecurity/37271.html

9. *July 14, Government Executive* — **OMB steps up data security reporting requirements.** In an effort to improve the federal response to data breaches putting personal information such as Social Security numbers at risk, the Office of Management and Budget (OMB) is eliminating the distinction between suspected and confirmed breaches for reporting purposes. In a Wednesday, July 12 memorandum, Karen Evans, administrator of OMB's Electronic Government and Information Technology division, said that agency chief information officers should not hold back reporting suspected breaches, both electronic and physical, to the Homeland Security Department's computer emergency readiness team, known as US−CERT. The memo says that all security incidents involving such information must be reported within an hour. US−CERT reporting guidelines for federal agencies already require reporting within one hour for any incidents involving unauthorized electronic or physical access to federal systems or data. An agency now will have to report incidents of improper usage within an hour. Previously, the requirement was one week. The memo also reiterates requirements established in February 2000 for detailing security funding in information technology budgets. In addition to those requirements, the memo asks agencies to provide additional details on resources they devote to fixing security weaknesses, as part of their fiscal 2008 budget requests.
Source: http://www.govexec.com/story_page.cfm?articleid=34555&dcn=to daysnews

10. *July 14, Websense Security Labs* — **Phishing Alert: IberCaja bank.** Websense Security Labs has received reports of a new phishing attack that targets customers of the Spanish Bank, IberCaja. Users receive a spoofed e−mail message, which claims that the bank has detected an error in their personal information and has deactivated online banking services, pending user

verification of the information. Users are instructed to click on a link contained in the e−mail to log in to their account. They are then taken to a phishing site that requests their login ID, password, and other logon details.
Source: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =552

11. *July 12, Wired* — **Hacker spawns a French Watergate.** A hack of a Luxembourg bank's records is emerging as a key detail of the so−called Clearstream affair, a national scandal that's pulled top−level politicians, powerful corporate executives, and now a white−hat hacking group into its orbit. At the heart of the storm is a sophisticated conspiracy to falsely implicate a number of celebrities, high−ranking officials, and political candidates in a bribery scandal. Among the falsified evidence produced by the conspirators before the fraud unraveled were confidential bank records originating with the Clearstream bank in Luxembourg, which were expertly modified to make it appear that some French politicians had secretly established offshore bank accounts to receive bribes. The falsified records were then sent to investigators, with enough authentic account information left in to make them appear credible.
Source: http://www.snpx.com/cgi−bin/news55.cgi?target=150757747?−262 2

[Return to top]

Transportation and Border Security Sector

12. *July 17, Boston Globe* — **Another key Big Dig connector shut.** Yet another crucial link between Interstates 90 and 93 in the heart of Boston has been closed after inspectors found about 40 potentially dangerous bolt fixtures similar to the ones suspected in last Monday's (July 10) fatal tunnel ceiling collapse, said state officials. Needed repairs and safety checks to the entire Big Dig project could take two months or more, Massachusetts Governor Mitt Romney said, adding that the bolt−and−epoxy ceiling fasteners throughout the tunnel system represent a "systemic failure, not an anomaly or a fluke." Officials are urging commuters to take public transportation, alternate routes, or seek staggered work hours. Drivers can expect significant delays, said Acting Boston Transportation Commissioner Thomas J. Tinlin, especially those headed to the South Boston waterfront near the Seaport area and World Trade Center. Tinlin also said that drivers throughout the city might notice that traffic signals on their usual route will take longer to change. While motorists try to figure out new ways to get to work and run errands, federal and state investigators are trying to determine what went wrong when the passenger was killed and whether anyone should be held criminally responsible.
Source: http://www.boston.com/news/traffic/bigdig/articles/2006/07/17/another_key_connector_shut/

13. *July 17, Associated Press* — **CSX freight train derails in Maryland.** One car of a CSX freight train has derailed near Brunswick, MD. CSX spokesperson Robert Sullivan says no one was hurt in the incident. The Maryland Transit Administration says it expects the track to be closed at least through Monday evening's rush hour −− which could cause delays for MARC commuters on the Brunswick line. MARC trains already are operating at 20 miles an hour below their normal speed due to heat restrictions.
Source: http://www.wjla.com/news/stories/0706/345195.html

14. *July 17, Associated Press* — **Missouri Amtrak riders spend part of their trip on bus.** Construction along the railroad tracks used by Amtrak in Missouri has forced the company to ferry passengers onto buses for part of their trips this summer. Union Pacific is spending $32 million to repair and improve track between Kansas City and St. Louis, and sometimes the Amtrak train cannot get around the heaviest construction work. Amtrak used buses for at least one leg on about half its trips between Kansas City and St. Louis in June, according to the Missouri Department of Transportation. Most trips that require bus rides occur in the morning, when Union Pacific crews are replacing ties, spreading rock under the tracks, or improving the surfaces at road crossings. Amtrak believes that the Union Pacific projects will eventually be a benefit, by providing its rail passengers with a smoother ride and faster travel times. Missouri transportation officials warn that more delays can be expected as construction continues through October.
Source: http://www.kansascity.com/mld/kansascity/news/local/15057784 .htm

15. *July 17, CBS News (NY)* — **New York's 'A' train loses power.** About 300 passengers were stranded on an 'A' Train in the Rockaway section of Queens Monday afternoon, July 17. Approximately 50 feet of the train's third rail buckled, causing it to lose power on an overpass east of Cross Bay Bridge. Because of the extreme heat, New York City firefighters and a number of ambulances rushed to the scene. Firefighters helped passengers out of the door at the rear of the train and used ladders to help them from the overpass.
Source: http://wcbstv.com/topstories/local_story_198145730.html

16. *July 17, Associated Press* — **Northwest, flight attendants in deal.** The union that represents Northwest Airlines Corp. flight attendants said it has tentatively agreed to deep wage cuts and work rule changes on Monday, July 17, the same day the airline had bankruptcy court clearance to impose a new contract that had drawn strike threats. The union didn't release details of the agreement, which is subject to a vote by union members. But Northwest would get the $195 million in annual savings it had been looking for under the pact, according to Danny Campbell, interim vice president of the Northwest branch of the Association of Flight Attendants. "With the airline in bankruptcy, this deal was always going to be about survival," said Mollie Reiley, interim president of the Northwest branch of the union.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/17/AR2006071700404.html

17. *July 16, Aviation Now* — **Coast Guard wants UAVs to close gap in maritime air patrol hours.** The U.S. Coast Guard is hoping unmanned aerial vehicles (UAVs) will help close the operational gap in its maritime air patrols, a top agency official says. Current Coast Guard legacy aircraft fly 44,400 marine patrol aircraft (MPA) flight hours per year, well short of the agency's target of 61,600 MPA flight hours, says Rear Adm. Wayne Justice, the Coast Guard's Assistant Commandant for Response. The Coast Guard plans to narrow that gap by 2012 with new aircraft and ship−launched unmanned aerial vehicles (UAVs) acquired through the long−term Deepwater recapitalization program. Deepwater calls for the procurement of 45 Eagle Eye Vertical Unmanned Aerial Vehicles as well as high altitude endurance UAVs. In addition, the land−based high altitude UAVs, capable of flying more than 30 hours without refueling and loitering in an area far longer than manned aircraft, will significantly improve Coast Guard maritime domain awareness, Justice told a July 13 Senate Commerce Committee hearing on UAVs. The hearing explored using Alaska and the Pacific region's airspace to

integrate UAVs into the National Airspace System.
Source: http://www.aviationnow.com/avnow/news/channel_aerospacedaily_story.jsp?id=news/CUAV07176.xml

[Return to top]

Postal and Shipping Sector

18. *July 14, Memphis Business Journal (TN)* — **FedEx subpoenaed, says isn't being investigated.** FedEx Corp. was subpoenaed to testify before a grand jury as part of an investigation into violations of antitrust laws in its industry. Reuters and the Associated Press report that the package shipper has received the subpoena in connection with a U.S. Justice Department probe for possible criminal violations of antitrust laws in the air−cargo industry, including alleged price−fixing. FedEx officials told Reuters they do not believe the Memphis−based company is a target of the investigation and that it is cooperating with the investigators.
Source: http://biz.yahoo.com/bizj/060714/1316193.html?.v=1

[Return to top]

Agriculture Sector

19. *July 17, Agricultural Research Service* — **Microbes to fight wheat fungus.** Four yeasts and three bacteria that live on flowering wheat heads, but cause no harm there, have been patented by the U.S. Department of Agriculture (USDA) as biological control agents in the fight against Fusarium head blight (FHB). Caused by the fungus Fusarium graminearum, FHB is among the most costly diseases of cereal crops worldwide, including wheat, barley and oats. From 1998 to 2000, FHB epidemics in U.S. small grains inflicted an estimated $2.7 billion worth of losses. The fungus infects wheat through its flower tissues, including anthers. But competition for space and nutrients there is fierce, according to studies by Agricultural Research Service scientists. Indeed, some of the bacteria and yeasts that the researchers isolated from wheat anthers secrete antibiotics, or use other means, to keep the fungus at bay. To exploit this "natural antagonism," scientists devised fermentation procedures to culture quantities of the beneficial microbes for application to flowering wheat heads.
Source: http://www.ars.usda.gov/News/docs.htm?docid=1261

20. *July 14, U.S. Department of Agriculture* — **Animal disease crisis management center launched.** The U.S. Department of Agriculture (USDA) will send four veterinary specialists to Rome, Italy, to assist the United Nations' Food and Agriculture Organization (FAO) in launching a new crisis management center that will enhance worldwide response to animal disease. The Center will begin operations by the end of July at FAO's Rome headquarters. The Crisis Management Center, a facility run by the FAO in close collaboration with the World Organization for Animal Health will provide animal disease analysis and information and deploy international resources to prevent and contain dangerous animal diseases. The current focus will be on highly pathogenic H5N1 avian influenza that continues to spread throughout the world. The U.S. will provide $1.8 million to FAO to create the Center. Other contributors include France, Germany, Italy, the Netherlands, and the United Kingdom.

Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/07/0251.xml

[Return to top]

Food Sector

21. *July 17, Associated Press* — **Man arrested for tainting juice.** Five months after juice spiked with dishwashing soap sickened more than 40 people during a church communion service, police on Monday, July 17, arrested an employee of the store where the juice was purchased. Wendell Woodroffe was charged with 22 counts of assault and 22 counts of assault of a victim 60 or older, said Darien, CT, police Lt. Ron Bussell. More than 40 people became ill during a communion service February 5 at Calvary Baptist Church in Darien, and five were treated at hospitals for nausea and vomiting. People who drank the juice reported a burning sensation in their throats. Woodroffe also was charged in a previously unreported incident involving alleged tampered with prune juice that sickened a Darien woman in December. That incident came to light after the church illnesses, Bussell said.
Source: http://www.washingtonpost.com/wp-dyn/content/article/2006/07/17/AR2006071700438.html

[Return to top]

Water Sector

22. *July 17, Agence France-Presse* — **Kemira buys Cytec industries' water treatment chemical operations.** Kemira said it has acquired the water treatment chemical operations of U.S. firm Cytec Industries for $238 million. As part of the deal, Kemira has bought five production plants in the U.S., the Netherlands and the United Kingdom.
Source: http://www.forbes.com/business/feeds/afx/2006/07/17/afx28822 86.html

23. *July 17, Associated Press* — **Flight camera to check for chemical leaks.** A helicopter equipped with a special camera will fly over Louisiana waterways and industrial plants in a search for chemical leaks. The camera uses a technique that displays chemical leaks as black, inky clouds. The state Department of Environmental Quality (DEQ) used the camera last year in the Baton Rouge area to look for leaks suspected to be adding to the areas problem with ozone pollution. Bruce Hammatt, DEQ administrator and technical adviser, says this week's flights are the first of four scheduled for this year. The first will focus on possible leaks and releases from barges and other marine traffic. The flights will concentrate on the Mississippi River from Baton Rouge to New Orleans, the Gulf Intracoastal Waterway and along the Calcasieu River.
Source: http://www.wafb.com/Global/story.asp?S=5158887

[Return to top]

Public Health Sector

24. *July 17, Agence France−Presse* — **Singapore to hold large−scale flu pandemic exercise.** Singapore will simulate a flu pandemic on July 21 and July 22 in a large−scale exercise involving Changi Airport, a border crossing to Malaysia and several hospitals, the government has said. More than 1,000 health workers and public servants from other agencies will take part along with about 500 volunteer "patients", the Ministry of Health said on Monday, July 17. The exercise at 19 locations is based on an avian influenza infection among humans and simulates an escalation of the flu pandemic in Singapore. There will be a simulated surge of flu patients at participating medical clinics. Other volunteers at the air and land crossings will pretend to be patients or to have been in close contact with flu sufferers.
Source: http://news.yahoo.com/s/afp/20060717/hl_afp/healthflusingaporeexercise_060717114141;_ylt=AokMcYSIbBup__Qy2NY43c2JOrgF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

25. *July 14, CBC News (Canada)* — **Saskatchewan man develops anthrax in quarantine area.** A man in Saskatchewan, Canada, has developed skin anthrax in the midst of the largest outbreak of the disease among livestock in the province's history. The man is being treated with antibiotics and is expected to recover fully. Cutaneous or skin anthrax is the most common and least serious form of the disease. Government officials who are investigating the suspicious deaths of 149 livestock in Saskatchewan have quarantined 36 farms as of Friday, July 14, because of the anthrax outbreak. Most of the farms under quarantine are in the Melfort area, northeast of Saskatoon, and around Wynyard, north of Regina.
Source: http://www.cbc.ca/canada/saskatchewan/story/2006/07/14/anthr ax−man.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

26. *July 17, Providence Journal (RI)* — **Rhode Island acts to solve communications problems.** As Hurricane Bob roared into Rhode Island, high winds ripped down power lines, knocked out radio communications and left rescue workers with no way to talk to each other. That was 15 years ago. In some ways, not much has changed. There's a spider web of communications systems throughout the state for public safety and government officials. The majority of police and fire departments are on systems that use various radio frequencies, which are incompatible with other departments, and can lose a signal once rescuers are out of their municipalities or even inside buildings. To call other departments, many rely on cell phones and walkie−talkie−like Nextel phones, which are useless if cell towers are knocked down. In other ways, much has changed. The state has a variety of communications weapons at its disposal if a hurricane strikes this season, including the interoperable 800 MHz radio system, the new state Emergency Operations Center that will allow state officials to oversee disaster response around the state, laptop computers so local emergency management directors are connected by Internet to the state center, and, as a last line of defense, amateur radio operators to relay messages for

state and local officials.
Source: http://www.projo.com/news/content/projo_20060717_chat17.17ef b6e.html

27. *July 17, Federal Emergency Management Agency* — **Federal Emergency Management Agency National Situation Update.** California Wildfire Update Monday, July 17: The Sawtooth Fire (62,000 acres) has merged with the Millard Fire (15,572 acres) and the Heart Fire (800 acres). The combined fire/complex has consumed 78,372 acres. Combined containment is reported at 60 percent. 1,500 residences, 1,500 outbuildings and/or other structures, and 50 commercial properties remain threatened. Canyon Fire: 31,933 acres at 75 percent contained. This fire is 11 miles west of Patterson, CA. Several residences, ranches, rangelands, watersheds remain threatened. Very active fire behavior was reported.
Tropical Activity: Eastern Pacific: Tropical Depression Carlotta continues its downward trend and expected to dissipate in 36 to 48 hours. Tropical Depression 5−E is moving West at 15 mph, away from the west coast, and is expected to become a hurricane in 24 to 48 hours. These tropical cyclones do not pose a threat to the U.S. or its territories.
To view other Situation Updates: http://www.fema.gov/emergency/reports/index.shtm
Source: http://www.fema.gov/emergency/reports/2006/nat071706.shtm

28. *July 17, Department of Homeland Security* — **Department of Homeland Security launches updated emergency preparedness Website.** The tornados, flooding and wildfires recently experienced in parts of the country are another reminder of how critical it is for Americans to prepare for emergencies. The Department of Homeland Security's Ready Campaign Monday, July 17, launched an updated version of its Website, www.ready.gov, to educate Americans about the simple steps they should take to be ready for a variety of emergencies.
For more information: http://www.ready.gov/
Source: http://www.dhs.gov/dhspublic/display?content=5744

29. *July 17, Department of Homeland Security* — **Department of Homeland Security to sponsor Third Annual National Preparedness Month.** For the third straight year, the Department of Homeland Security will sponsor National Preparedness Month, along with a coalition of more than 200 national, regional, state and local organizations. National Preparedness Month is a nationwide effort held each September to encourage Americans to prepare for emergencies in their homes, businesses and schools. This year's goals are to increase public awareness about the importance of family emergency preparedness and to urge individuals to make themselves and their loved ones better prepared. National Preparedness Coalition membership is open to all public and private sector organizations. Groups can register to become a National Preparedness Month Coalition member by visiting the ready.gov Website and clicking on the National Preparedness Month banner.
Ready Website: http://www.ready.gov/
National Preparedness Month Coalition Partners:
http://www.dhs.gov/dhspublic/interapp/press_release/press_re lease_0959.xml
Source: http://www.dhs.gov/dhspublic/display?content=5745

30. *July 16, Providence Journal (RI)* — **Rhode Island official frets over massive power line damage during hurricane.** Should a major hurricane strike Rhode Island, Robert Warren, head of the Rhode Island's Emergency Management Agency, says he's most worried about a sustained loss of electric power to homes and businesses. Every utility, every hospital and

nursing home, every police and fire station in Rhode Island has prepared emergency plans and backup power sources to keep operating if a hurricane knocks out electric lines. But Rhode Island's link to modern comforts is very tenuous. Warren fears the state's heavy coverage of trees in inland towns and its dense development, especially along the coast, will cause massive power line damage. "I really think we'll have areas of the state without power for a month," Warren says at nearly every meeting of emergency responders. Two weeks ago, Warren mailed letters to the state's 39 cities and towns, asking them to identify critical sites, such as police and fire stations, that need backup generators. The Army Corps of Engineers can supply generators for key sites and routinely it is called in following a disaster. Warren is trying to jump−start the process by asking the Army to assess each site now so the equipment can be set up faster when needed.
Source: http://www.projo.com/news/content/projo_20060716_power16.16a 0a16.html

31. *July 14, South Florida Business Journal* — **Business continuity center opens in Florida.** Miami−Dade County, FL, has inaugurated a Business Continuity Resource Center. The facility was created to allow companies to continue operating in the event of an emergency or natural disaster such as a hurricane. Designed to withstand up to a Category 5 hurricane, the county said the building has secure sustained communications, worldwide connectivity, an uninterrupted power supply, business services and applications, monitoring and backup services and work stations.
Source: http://phoenix.bizjournals.com/southflorida/stories/2006/07/ 10/daily46.html

32. *July 13, Federal Emergency Management Agency* — **President declares major disaster for Virginia.** The head of the Department of Homeland Security's Federal Emergency Management Agency announced Thursday, July 13, that federal disaster aid has been made available for Virginia to supplement Commonwealth and local recovery efforts in the area struck by severe storms, tornadoes, and flooding during the period of June 23 to July 6, 2006.
For more information: http://www.fema.gov/news/event.fema?id=6585
Source: http://www.fema.gov/news/newsrelease.fema?id=27758

[Return to top]

Information Technology and Telecommunications Sector

33. *July 17, IDG News Service* — **Hackers learn from open source.** Hackers are taking a page from the open−source playbook, using the same techniques that made Linux and Apache successes to improve their malicious software, according to McAfee Inc. Nowhere is this more apparent than within the growing families of "bot" software. Unlike viruses of the past, bots tend to be written by a group of authors, who often collaborate by using the same tools and techniques as open source developers, said Dave Marcus, security research and communications manager with McAfee's Avert Labs. The current generation of bot software has grown to the point where open−source software development tools make a natural fit. With hundreds of source files now being managed, developers of the Agobot family of malware, for example, are using the open−source Concurrent Versions System software to manage their project.
Source: http://www.infoworld.com/article/06/07/17/HNhackerslearnfrom opensource_1.html

34. *July 17, VNUNet* — **U.S. plugs in 10.4 million broadband lines in 2005.** The Federal Communications Commission (FCC) has reported a 32 percent increase in the number of U.S. broadband subscribers during 2005. Total broadband Internet connections across the country increased by 10.4 million lines in 2005, according to the organization, and VoIP use is expected to more than triple. The FCC redefined broadband or high−speed lines on June 30, 2005 as services that deliver connection speeds in excess of 200 Kbps in at least one direction. This definition was expanded to include advanced service lines where connection speeds exceed 200 Kbps in both directions. This clarification allows for more detailed data collection regarding broadband penetration and trends.
Source: http://www.vnunet.com/vnunet/news/2160485/plugs−million−broa dband−lines

35. *July 14, TechWorld* — **Invisible rootkit heralds trouble ahead.** Security researchers have discovered a new type of rootkit they believe will greatly increase the difficulty of detecting and removing malicious code. The rootkit in question, called Backdoor.Rustock.A by Symantec and Mailbot.AZ by F−Secure, uses advanced techniques to avoid detection by most rootkit detectors. The rootkit is "unique given the techniques it uses," Symantec's Elia Florio wrote in a recent analysis. "It can be considered the first−born of the next generation of rootkits."
To read more of Florio's analysis:
http://www.symantec.com/enterprise/security_response/weblog/2006/06/raising_the_bar_rustocka_advan.html
Source: http://www.techworld.com/security/news/index.cfm?newsID=6453 &pagtype=all

36. *July 14, eWeek* — **Researchers in China claim to have cracked Skype Protocol.** A claim that a group of researchers in China has successfully cracked the Skype Protocol has set the blogosphere alight, but the company says there is no evidence that the software has been reverse−engineered. "We have no evidence to suggest that this is true. Even if it was possible to do this, the software code would lack the feature set and reliability of Skype," said the company. According to Charlie Paglee, CEO of VoIP startup Vozin Communications, in Fremont, CA, engineers at a small research outfit in China have cracked Skype's proprietary protocol to create a third−party application capable of connecting to Skype's 100 million users. Paglee announced the news on his blog on Friday, July 14, and posted screenshots of Skype connecting directly to a rudimentary application. Paglee, who tested the connection during two voice calls with the Chinese group, noted that his IP address was "100 percent correct" on the third−party software.
Paglee's blog: http://www.voipwiki.com/blog/
Source: http://www.eweek.com/article2/0,1895,1989301,00.asp

37. *July 12, ZDNet (UK)* — **PlusNet admits human error in e−mail disaster.** A large number of subscribers to the Internet service provider PlusNet have experienced a serious outage of their e−mail services, which also seems to have led to thousands of e−mails being erased. According to The Register, which first reported the story, over 700 GB of data was lost. It appears the problem was caused when a senior engineer mistook the management interface of a live e−mail server for that of a backup server, and erased all the data on the wrong one.
Source: http://news.zdnet.co.uk/communications/broadband/0,39020342, 39278586,00.htm

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of multiple vulnerabilities in Microsoft Internet Explorer (IE) 6.0. US−CERT is also aware of a public blog that will be posting new web browser bugs on a daily basis in July. US−CERT will be analyzing relevant vulnerabilities, as well as actively monitoring the site to provide additional information as it becomes available. Please review URL: http://metasploit.blogspot.com/2006/07/month−of−browser−bugs .html

US−CERT strongly recommends the following:

Review VU#159220 / Microsoft Internet Explorer vulnerable to heap overflow via the HTML Help Control "Image" property : http://www.kb.cert.org/vuls/id/159220

Disable ActiveX as specified in the following:

Securing Your Web Browser:
http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer

Malicious Web Scripts FAQ:
http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

Do not follow unsolicited links.

Review the steps described in Microsoft's document to improve the safety of your browser: http://www.microsoft.com/athome/security/online/browsing_saf ety.mspx

US−CERT will continue to update current activity as more information becomes available.

Public Exploit Code for Unpatched Vulnerabilities in Microsoft Internet Explorer

US−CERT is aware of publicly available exploit code for two unpatched vulnerabilities in Microsoft Internet Explorer. By persuading a user to double click a file accessible through WebDAV or SMB, a remote attacker may be able to execute arbitrary code with the privileges of the user. US−CERT is tracking the first vulnerability as VU#655100: http://www.kb.cert.org/vuls/id/655100

The second issue is a cross domain violation vulnerability that is being tracked as VU#883108: http://www.kb.cert.org/vuls/id/883108

Until an update, patch, or more information becomes available, US−CERT recommends the following:

Do not follow unsolicited links.

To address the cross domain violation vulnerability (VU#883108):
http://www.kb.cert.org/vuls/id/883108

Disable ActiveX as specified in the Securing Your Web Browser:
http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer

Review Malicious Web Scripts FAQ:
http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

US−CERT will continue to update current activity as more information becomes available

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT.
http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	44139 (−−−), 1026 (win−rpc), 38566 (−−−), 24232 (−−−), 35830 (−−−), 80 (www), 6999 (iatp−normalpri), 445 (microsoft−ds), 54856 (−−−), 25 (smtp) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

38. *July 17, Associated Press* — **Heat wave has much of nation sizzling.** Temperatures soared into the upper 90s and higher Sunday, July 16, from coast to coast, and choking heat is

expected to continue for the next few days, meteorologists said, as hot air is moving toward the East Coast. Illinois Governor Rod Blagojevich said Sunday the state would make more than 130 office buildings available as cooling centers beginning Monday, July 17. Minnesota Governor Tim Pawlenty ordered the National Guard out to help firefighters as temperatures even in the normally cool northern part of the state pushed 100 degrees amid very dry conditions. The National Weather Service issued excessive heat warnings for Las Vegas, Chicago, St. Louis, Philadelphia, Tulsa, OK., and parts of New Jersey, where thermometers made it into the 90s Sunday and were expected to reach 100 degrees Monday, July 17. Officials in Chicago, where a 1995 heat wave killed 700 people, opened 24−hour cooling centers and pleaded with people to check on elderly neighbors. South Dakota posted some of the nation's highest temperatures with a reading Saturday, July 15, of 115 at Pierre, the state capital, and an unofficial report of 120 outside the town of Usta in the state's northwest corner.
Source: http://hosted.ap.org/dynamic/stories/H/HEAT_WAVE?SITE=MIDTF&SECTION=HOME&TEMPLATE=DEFAULT

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer